УДК 681.3.06

КРИПТОАНАЛИЗ ПРЯМОЙ АТАКИ НА УНИВЕРСАЛЬНОЕ СЕМЕЙСТВО ХЕШ-ФУНКЦИЙ С АЛГЕБРАИЧЕСКИМ КОДИРОВАНИЕМ

к.т.н. Г.З. Халимов, А.Ю. Иохов, к.т.н. А.В. Северинов
(представил д.т.н., проф. Ю.В. Стасев)

Рассмотрены прямые атаки на MAC коды с алгебраическим кодированием. Получены аналитические выражения для вероятности навязывания по значению MAC кода и навязывания по ключу.

Введение. Практические схемы вычисления MAC кодов должны включать классы хеш-функций с большим коэффициентом сжатия для данных возможно очень большого объема. Для этих целей интерес представляют семейства хешей на основе длинных алгеброгеометрических кодов (АГК). Свойства таких схем хеширования и их модификации рассмотрены в ряде работ [1, 2]. Требования к параметрам MAC конструкций с алгеброгеометрическими кодами определяются оценками их стойкости к основным криптоаналитическим атакам.

Задачей статьи является криптоанализ MAC кодов с АГ кодами. С этой целью в разделе 1 приводятся основные определения и требования безопасности к кодам аутентификации сообщений. В разделе 2 получены оценки сложности прямой атаки на универсальное семейство хеш-функций с кодовыми схемами.

1. Определения и требования безопасности к кодам аутентификации сообщений. В представлении Принеля [3] MAC код есть функция отображения $h: K \times M \to R$, где пространство ключей $K = \{0,1\}^k$, пространство сообщений $M = \{0,1\}^*$ и пространство MAC значений $R = \{0,1\}^n$ для $k, n \geq 1$. Для заданных значений ключа $k \in K$ и сообщения $X \in M$, функция производит MAC значение $Y \in R$.

Противник подделает сообщение для MAC кода h, если, не зная случайный ключ k, он способен произвести новое сообщение X и MAC значение Y такое что $h(k,X) = Y$.

Определение 1. MAC код $h: K \times M \to R$ является $(t;\varepsilon;q)$-секретным, если, при случайно взятом ключе k, противник не может подделывать новое сообщение за время t с вероятностью лучше чем ε даже если ему

представлены значения q MAC кодов других сообщений по его выбору.

Большинство MAC кодов – это итеративные конструкции, которые используют функцию сжатия f, предварительное разбиение данных X на подблоки X_i и связку по обратному входу промежуточных результатов вычислений хеш-значений.

Обобщенная модель итеративного MAC кода для t подблоков определяется следующим алгоритмом итеративных вычислений:

$$H_0 = IV_k;$$
$$H_i = f_k(H_{i-1}, X_i) , 1 \le i \le t;$$
$$h(k,X) = g_K(H_t).$$

Секретный ключ k может использоваться в векторе инициализации IV, в функции сжатия f, и в выходном преобразовании g.

Конструктивными элементами MAC кодов на основе семейств хеш-функций являются хеш-функции, функции сжатия и итерационные хеш-функции. Основные определения и свойства хеш-функции приведем в представлении Рогавея [4].

Определение 1 [4]**.** Хеш-функцией называется функция отображения h: D → R , где область значений D = {0,1}*, а R = $\{0,1\}^n$ для некоторого n ≥ 1.

Определение 2 [4]**.** Функцией сжатия называется функция отображения f: D → R, где D = $\{0, 1\}^a \times \{0,1\}^b$ и R = $\{0,1\}^n$ для некоторых a, b, n ≥ 1 и a + b ≥ n.

Определение 3 [4]**.** Итерационной хеш-функцией от функции сжатия f: ($\{0,1\}^n \times \{0,1\}^b$) → $\{0,1\}^n$ является хеш-функция h: ($\{0,1\}^b$)* → $\{0,1\}^n$ определенная h (X_1 ... X_t) = H_t, где $H_i = f(H_{i-1}, X_i)$ при $1 \le i \le t$ (H_0 = IV).

Определяющими требованиями к хеш-функциям являются их стойкость к вычислению прообраза, второго прообраза, а также стойкости к коллизиям.

Определение 4 **(Стойкость к вычислению прообраза)** [5]**.** Хеш-функция h: $\{0,1\}^*$ → R является стойкой к вычислению прообраза силой (t, є), если не существует вероятностного алгоритма I_h, с входными значениями Y Є $_R$ R и значениями на выходе X Є {0,1}*, временем выполнения не более чем t, где h (X) = Y и вероятностью не менее є, оцененной при случайном выборе Y и I_h.

Стойкость хеш-функций к вычислению прообраза имеет важное значение для систем аутентификации, использующих хэш-значения паролей и секретных ключей.

Определение 5 **(Стойкость к вычислению второго прообраза)** [5]**.** Пусть S – конечное подмножество {0,1}*. Хеш-функция h: {0,1}*→ R является стойкой к вычислению второго прообраза силой (t, є, S), если

не существует вероятностного алгоритма S_h, с $X \in_R S$ и $X' \in \{0,1\}^*$, временем выполнения не более чем t, где $X' \neq X$ и $h(X') = h(X)$ и вероятностью не менее ϵ, оцененной при случайном выборе X и S_h.

Стойкость хеш-функций к вычислению второго прообраза определяет безопасность систем аутентификации с цифровой подписью.

Определение 6 **(Стойкость к коллизиям).** [5]**.** Хеш-функция $h: \{0,1\}^* \rightarrow R$ является стойкой к коллизиям силой (t, ϵ), если не существует вероятностного алгоритма C_h с известными выходными значениями X, $X' \in \{0,1\}^*$, временем выполнения не более чем t, где $X' \neq X$ и $h(X) = h(X')$ и вероятностью не менее ϵ, оцененной при случайном выборе C_h.

Определение 7. Хеш-функция называется простой или слабой если является стойкой к вычислению прообраза и стойкой к вычислению второго прообраза.

Определение 8. Хеш-функция называется сильной если является стойкой к вычислению прообраза, стойкой к вычислению второго прообраза и стойкой к коллизиям.

Определение сильной хэш-функции показывает, что вычислительно невозможно найти какую-либо коллизию и защищает против класса атак, известных как атака «день рождения».

Основными целями атак на функции выработки MAC кодов являются следующие:

1) нахождение корректной пары прообраза и MAC $(x, h(x,k))$ по одной или более заданным корректным парам $(x_i, h(x_i,k))$ для любого $x \neq x_i$ при неизвестном секретном ключе k;

2) нахождение неизвестного сеансового ключа k по одной или более заданным корректным парам прообразов и кодов аутентификации $(x_i, h(x_i,k))$.

Результаты работы криптоаналитика могут иметь различные последствия:

– *экзистенциальная подделка*. Нарушитель может определить значение кода подлинности сообщений, по крайней мере, для одного текста. Поскольку он не имеет контроля над текстом, такая подделка приводит к случайному характеру воздействия на систему управления;

– *избирательная подделка*. Злоумышленник может определить значение MAC кода для специфического текста, выбранного априорно. Практические атаки часто требуют, чтобы подделка была поддающаяся проверке. Это означает, что нарушитель знает, что подделанный код подлинности сообщений может быть принят за правильный с вероятно-

стью близкой к единице;

– *ключевое восстановление*. Нарушитель может определить секретный ключ k. Такой взлом более опасный, чем экзистенциальная подделка, так как это позволяет создавать произвольные избирательные подделки.

Как правило, адаптивная атака с выбором текста на практике трудно выполнима. Тем не менее, следует потребовать, чтобы алгоритмы кода подлинности сообщений были устойчивыми к самым сильным из возможных атак.

Атаки на функции MAC могут выполняться при следующих условиях:

1) атака с известным текстом – злоумышленнику заданы только одна или несколько корректных пар прообразов и кодов аутентификации $(x_i, h(x_i, k))$;

2) атака с выбираемым текстом – злоумышленник имеет возможность получить корректные пары $(x_i, h(x_i, k))$ для выбранных значений x_i (атака на нахождение ключа);

3) атака с адаптивным выбором текста – злоумышленник может получить корректные пары $(x_i, h(x_i, k))$ для любых x_i, выбранных в зависимости от результатов предшествующих запросов (атака с целью нахождения ключа).

Все атаки можно разделить на две группы: атаки, базирующиеся на уязвимости алгоритма преобразований (аналитические) и атаки, независящие от алгоритма.

Лучшие известные атаки на коды аутентификации сообщения рассмотрены в [3].

Угадывание кода подлинности сообщений (Guessing of the MAC). Прямая атака на алгоритм MAC код состоит в выборе произвольного нового сообщения, и впоследствии угадывание значения кода подлинности сообщений. Это может быть сделано двумя способами: или угадывание MAC кода непосредственно с вероятностью успеха 2^{-n} или угадывание ключа, с последующим вычислением значения MAC кода, с вероятностью успеха 2^{-k}. Здесь n обозначает размер в битах значения MAC кода и k размер в битах секретного ключа. Это – атака неподдающаяся проверке: нарушитель не знает априорно, было ли его угадывание правильным. Выполнимость атаки зависит от числа испытаний, которые могут быть выполнены и ожидаемого значения успеха.

Исчерпывающий поиск ключа (Exhaustive Key Search). Это – другая прямая атака, которая может применяться к любому алгоритму. Атака требует приблизительно k/n известных пар текста – MAC для данного

ключа; пытаясь определить ключ, пробуя один за другим все ключи. Ожидаемое число испытаний равно $2^{\kappa - 1}$. В отличие от предыдущей атаки, эту атаку выполняют вне сеанса связи (off-line), и это приводит к взлому MAC алгоритма.

Подделка основанная на внутренней коллизии (Internal Collision Based Forgery). Последствие этой атаки состоит в том, что если обнаружить внутреннюю коллизию (совпадение промежуточных результатов при вычислении значений MAC кодов), её можно использовать, для создания подделки MAC кода на отдельном выбранном тексте.

Preneel и van Oorschot [8] показали, что внутренняя коллизия для h функции может быть найдена, используя u известных пар текст – MAC и v выбранных текстов, где ожидаемые значения для u и v являются следующими соотношениями: $u = 2^{(l+1)/2}$ и $v = 0$ (здесь l, обозначает размер в битах связанной переменной), если выход преобразования MAC кода является перестановкой; иначе, v равно приблизительно

$$2[2^{l-n} + \lfloor (l-n)/(n-l) \rfloor + 1].$$

Дальнейшие оптимизации этой атаки возможны, если множество пар текст – MAC имеет общую последовательность из s последних блоков.

Ключевое восстановление на основе внутренней коллизии (Internal Collision Based Key Recovery). Для некоторых функций сжатия, можно расширить внутреннюю атаку коллизии к ключевой атаке восстановления [9]. Идея состоит в том, чтобы идентифицировать одну или более внутренних коллизий; например, если f не является перестановкой для фиксированного H_i, и внутренняя коллизия после первого блока сообщения определяется уравнением $f_K(H_0,X_i) = f_K(H_0,X_i')$ в котором K и возможно H_0 являются неизвестным (предполагается, что $H_0 = IV$ зависимы от ключа). Для некоторых функций сжатия f, можно получить информацию относительно секретного ключа, основанного на таких отношениях.

Атака методом декомпозиции (Divide-and-Conquer Attack). Эта атака является специальным случаем ключевого восстановления на основе внутренней коллизии. Для некоторых функций сжатия, которые используют два раздельных ключа, можно использовать внутренние коллизии для ключевого восстановления [6].

Пусть ключи обозначены K_1; K_2. Общая идея состоит в том, что нарушитель сначала ищет некоторые внутренние коллизии, затем методом исчерпывания определяет ключ K_1, который производит эти коллизии. Когда K_1 определен, исчерпывающий поиск используется, чтобы найти K_2. Поэтому, стойкость такого MAC кода зависит от его индивидуальных ключей, а не от их объединенной длины. Эта атака менее практична чем простой исчерпывающий поиск ключа, поскольку требуется

большое количество известных пар текст – MAC.

Подделка Exor (Exor Forgery). Этот тип подделки возможен, если значение H_i вычисляется как функция $H_{i-1} \oplus X_i$, и если нет никакого последующего преобразования хеш-выхода. Самый легкий вариант атаки требует только единственной известной пары текст – MAC. Предположим, что вход X и его дополняемая версия X' состоят из единственного блока. Если известно h(K,X), немедленно следует что

$$h(k,X \parallel (X \oplus h(k;X))) = h(k;X).$$

Таким образом можно создать новое сообщение с тем же значением MAC, которое является подделкой. Базовая CBC-конструкция использует вычисление $H_{i-1} \oplus X_i$ и оказывается уязвима к атаке exor-подделки.

Атаки на MAC коды, базирующиеся на уязвимости алгоритма преобразований, относятся к аналитическим. Они учитывают недостатки и криптоаналитические слабости хеш-функций, функций сжатия и итерационных хеш-функции, которые являются основными конструктивными элементами MAC кодов. К классу аналитических атак можно отнести атаку на базовый алгоритм шифрования. Так как алгоритмы шифрования разрабатывались как двунаправленные (поддерживают обратное преобразование), то это может увеличить уязвимость функций сжатия, базирующихся на блочных симметричных шифрах.

2. Оценка сложности прямой атаки на универсальное семейство хеш-функций с кодовыми схемами. Семейство хеш-функций (N;n,m) определяет MAC код как отображение

$$h: A \rightarrow B, \qquad (1)$$

где $h \in H$, $|H| = N$, $|A| = n$ и $|B| = m$, $n \geq m$.

Связь между универсальным семейством хеш-функций и кодовыми схемами устанавливает следующая теорема.

Теорема 1 [7]**.** Если существует $(N,K,D)_q$ код, тогда существует $(N - D)/N - U(N;K,q)$ универсальное семейство хеш-функций. Обратно, если $\varepsilon - U(N;n,m)$ хеш-семейство, тогда существует $(N,n,N(1-\varepsilon),m)$ код.

Рассмотрим основные атаки на MAC коды с кодовыми схемами.

Одна из первых атак на MAC коды – это прямая атака. Прямая атака состоит в выборе произвольного сообщения, и затем в угадывании значения кода подлинности сообщений. Это может быть сделано двумя способами: путем угадывания MAC кода непосредственно с вероятностью успеха $P_{уMAC}$ или угадывания ключа с вероятностью успеха $P_{ук}$. Вероятность успеха такой атаки будет определяться соотношением

$$P_у = \min\{P_{уMAC}, P_{ук}\}. \qquad (2)$$

Оценим значение вероятности успеха при прямой атаке.

Утверждение 1. Пусть $(n - d)/n - U(n;q^k,q)$ универсальное семейство хеш-функций, построенное с использованием $(n,k,d)_q$ кода, где $h(k,X) = c_X(k)$. Тогда вероятность поделки MAC кода с путем угадывания MAC значения при однократной попытке будет равна $P_{уMAC} = q^{-1}$.

Успех угадывания кода подлинности сообщений определяется равенством $h(k,X) = \beta$, где k-искомый ключ и β-выбираемое случайное значение из элементов кода принадлежащих полю F_q. Вероятность успеха такой атаки зависит только от размера поля представления символов кода и при случайном выборе значения β будет равна q^{-1}.

Утверждение 2. Пусть $(n - d)/n - U(n;q^k,q)$ универсальное семейство хеш-функций на основе $(n,k,d)_q$ кода, который не содержит кодовые слова $c(y) = \alpha 1(y)$, $\alpha \in F_q$ и $h(k,X) = c_X(k)$. Тогда вероятность угадывания MAC кода с помощью ключа при однократной попытке будет удовлетворять неравенству $P_{ук} \le (n - d)/n$.

Успех угадывания кода подлинности сообщений определяется равенством $h(k,X) = h(k',X)$, где k-искомый ключ и k'-выбираемый случайно из множества элементов кода. Вероятность успеха такой атаки будет зависеть от исходного сообщения и искомого ключа. Так как алгоритм MAC кодирования построен с использованием $(n,k,d)_q$ кода, который не содержит слова все символы которых равны константе α, тогда наибольшее число одних и тех же элементов $\beta \in F_q$ в кодовом слове не будет превышать значения $n - d$ и при случайном выборе ключа вероятность успеха не превысит значения $(n - d)/n$.

Расширим прямую атаку на MAC коды путем многократных попыток угадываний MAC значений и ключей. Анализ такой атаки обобщается в следующих утверждениях.

Утверждение 3. Пусть $(n - d)/n - U(n;q^k,q)$ универсальное семейство хеш-функций построенное с использованием $(n,k,d)_q$ кода, где $h(k,X) = c_X(k)$. Тогда вероятность поделки MAC кода с путем угадывания MAC значения при t кратной попытке будет равна $P_{уMAC}(t) = tq^{-1}$.

Пусть искомый MAC код равномерно распределен на множестве возможных значений. При t попытках угадывания формируются t различных MAC значений. Подделка MAC означает, что искомый MAC код окажется среди этих значений и вероятность этого события равна t/q.

Утверждение 4. Пусть $(n - d)/n - U(n;q^k,q)$ универсальное семейство хеш-функций на основе $(n,k,d)_q$ кода, который не содержит кодовые слова $c(y) = \alpha 1(y)$, $\alpha \in F_q$ и $h(k,X) = c_X(k)$. Тогда вероятность угадывания MAC кода с помощью ключа при t кратной попытке будет удовлетворять

неравенству

$$P_{\text{ук}}(t) \le \sum_{i=1}^{t} C_t^i C_{n-d}^i / (C_n^i C_{n-i}^{t-i}). \qquad (3)$$

Пусть искомый ключ MAC кода h(k,X) равномерно распределен на множестве возможных значений. При t попытках угадывания формируются t различных ключа и вычисляются MAC значения. Подделка MAC означает, что $h(k,X) = h(k_i,X)$, хотя бы для одного k_i, i = 1, … , t. Вероятность успеха атаки складывается из вероятностей однократного, двух кратного и т.д., t кратного угадывания ключа при t попытках. Так как ключи не повторяются, тогда с каждой попыткой подделки размер множества ключей будет уменьшаться на единицу. Наибольшее число одних и тех же элементов $\beta \in F_q$ в кодовом слове не будет превышать значения n – d и на каждом j шаге подделки это число в зависимости от успеха или неуспеха будет меняться от n – d до n – d – j. Получим выражение для оценки вероятности i кратного угадывания ключа при t попытках $P_{\text{усп i}}(t)$. Эта вероятность будет определяться как число сочетаний из t по i произведений вероятностей успешного угадывания и не угадывания. Вероятность успешного угадывания, в зависимости от того на каких шагах оно произошло, определяется отношением (n – d)(n – d – 1) … (n – – d + 1 – i)/($n_{j1}n_{j2}$ … n_{ji}), где n_{jk} – размер поля ключей для k шага. Вероятность не угадывания в свою очередь определяется отношением d(d – – 1) … (d + 1 – t + i)/($n_{s1}n_{s2}$ … $n_{s(t-i)}$), где n_{sr} – размер поля ключей для r шага. Значения n_{j1}, n_{j2}, … , n_{ji} и n_{s1}, n_{s2}, … , $n_{s(t-i)}$ принимают все значения от n до n – t + 1. Искомое выражение для вероятности i кратного угадывания ключа при t попытках будет иметь вид:

$$P_{yi}(t) = C_t^i (n-d)(n-d-1) \dots (n-d+1-i) d(d-1) \dots$$
$$\dots (d+1-t+i) / n(n-1) \dots (n-t+1)$$

или $$P_{yi}(t) = C_t^i C_{n-d}^i C_d^i / (C_n^i C_{n-i}^{t-i}).$$

И окончательно получим

$$P_{\text{ук}}(t) \le \sum_{i=1}^{t} P_{\text{усп i}}(t) = \sum_{i=1}^{t} C_t^i C_{n-d}^i C_d^i / (C_n^i C_{n-i}^{t-i}).$$

Модернизируем прямую атаку угадывания MAC значения с условием, что атака продолжается до первого угадывания. Предполагается, что можно контролировать результат успеха подделки. Оценим сложность такой атаки.

Утверждение 5. Пусть (n – d)/n – $U(n;q^k,q)$ универсальное семейство хеш-функций построенное с использованием $(n,k,d)_q$ кода, где $h(k,X) = c_X(k)$. Тогда граничное значение для среднего числа попыток пря-

мой атаки с угадыванием ключа до первого успеха равно $N_{MAC} = (q + 1)/2$.

Пусть искомый МАС код равномерно распределен на множестве возможных значений. Успех атаки определяется событием $h(k,X) = \beta$, где k-искомый ключ и β-выбираемое случайное значение из элементов кода принадлежащих полю F_q. Вероятность успеха атаки для i попытки будет определяться как произведение вероятности успешного угадывания на i-м шаге и вероятности не угадывания на предыдущих шагах. С учетом утверждения 2, первая вероятность определяется соотношением $1/(q - i)$, а вторая – как $(q - 1)(q - 2) \ldots (q - i)/[q(q - 1) \ldots (q - i + 1)]$. Отсюда вероятность успеха атаки для i попытки будет равна $1/q$ и среднее число попыток прямой атаки с угадыванием МАС значения до первого успеха определяется выражением $N_{MAC} = 1/q + 2/q + \ldots + q/q = (q + 1)/2$.

Утверждение 6. Пусть $(n - d)/n - U(n;q^k,q)$ универсальное семейство хеш-функций на основе $(n,k,d)_q$ кода, который не содержит кодовые слова $c(y) = \alpha 1(y)$, $\alpha \in F_q$ и $h(k,X) = c_X(k)$. Тогда граничное значение для среднего числа попыток прямой атаки с угадыванием ключа до первого успеха равно

$$N_K = \frac{n-d}{n} \sum_{i=1}^{d+1} C_d^{i-1} C_{n-1}^{i-1} . \qquad (4)$$

Пусть искомый ключ МАС кода $h(k,X)$ равномерно распределен на множестве возможных значений. Подделка МАС означает, что $h(k,X) = h(k_i,X)$ для ключа k_i сформированного на I шаге. Вероятность успеха атаки для i попытки будет определяться как произведение вероятности успешного угадывания на i-м шаге и вероятности не угадывания на предыдущих шагах. С учетом утверждения 1, первая вероятность определяется соотношением $(n - d)/(n - i)$, а вторая – как $d(d - 1) \ldots (d + 1 - - i)/[n(n - 1) \ldots (n + 1 - i)]$. Число попыток изменяется от 1 до d + 1. Отсюда среднее число попыток прямой атаки с угадыванием ключа до первого успеха определим как математическое ожидание числа попыток по распределению плотности вероятности успешного угадывания на i-м шаге

$$N = \frac{n-d}{n} + 2\frac{d(n-d)}{n(n-1)} + 3\frac{d(d-1)(n-d)}{n(n-1)(n-2)} + \ldots + (d+1)\frac{d(d-1)\ldots 1(n-d)}{n(n-1)(n-2)\ldots (d+1)},$$

что приводит к результирующему выражению.

Выводы. Впервые получены выражения для оценки сложности прямой атаки на МАС коды с универсальным хешированием и алгебраическим кодированием для подделок с угадыванием МАС значения и угадывания по ключу. Атака с угадыванием МАС значений является эквивалентной атаке на криптографические хеш-функции и менее эффектив-

ной по сравнению с атакой угадывания по ключу.

ЛИТЕРАТУРА

1. *Bierbrauer J., Johansson T.,Kabatianskii G., Smeets B. On families of hash functions via geometric codes and concatenation // Advances in Cryptology-CRYPTO '93 Proceedings. – Springer-Verlag, – 1994. – P. 331 – 342.*
2. *Халимов Г.З., Кузнецов А.А. Аутентификация с применением алгеброгеометрических кодов // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2001. – Вып. 120. – С. 103 – 109.*
3. *Preneel B. "Cryptographic primitives for information authentication state of the art." in State of the Art in Applied Cryptography (B. Preneel and V. Rijmen, eds.) // Lecture Notes in Computer Science. – Springer-Verlag. – 1998. – No. 1528. – P. 50 – 105.*
4. *Black J., Rogaway P. Ciphers with arbitrary finite domains // Proceedings of CT-RSA'02 (B. Preneel, ed.) // Lecture Notes in Computer Science Springer-Verlag. – 2002. – No. 2271. – P. 114 – 130,.– [Электр. ресурс]. – Режим доступа: www.cs.ucdavis.edu/~rogaway/papers/subset.htm.*
5. *Brown D.R.L. Generic groups, collision resistance, and ECDSA. – [Электр. ресурс]. – Режим доступа: http://eprint.iacr.org/2002/026/2002.*
6. *Preneel B., van Oorschot P.C. MDx-MAC and building fast MACs from hash functions // Proceedings of Crypto'95 (D. Coppersmith, ed.) in Lecture Notes in Computer Science. – Springer-Verlag. – 1995 – .No. 963 – P. 1 – 14. – [P. 150, 152].*
7. *Bierbrauer J., Johansson T., Kabatianskii G., Smeets B. On families of hash functions via geometric codes and concatenation // Advances in Cryptology-CRYPTO '93 Proceedings. – Springer-Verlag. – 1994. – P. 331 – 342.*

Поступила 24.11.2004

ХАЛИМОВ Геннадий Зайдулович, *канд. техн. наук, доцент кафедры ХУПС. В 1978 году окончил ХВВКИУ. Область научных интересов – теория аутентификации, алгебраическая теория кодов и их применение в системах передачи данных.*

ИОХОВ Александр Юрьевич*, адъюнкт ХУПС. В 2000 году окончил ХВУ. Область научных интересов – теория аутентификации, коды аутентификации с использованием теории смещенных и связных массивов и их применение в системах передачи данных.*

СЕВЕРИНОВ Александр Васильевич *канд. техн. наук, доцент, заместитель начальника кафедры Компьютерных систем ХУПС. В 1992 году окончил ХВУ. Область научных интересов – теория аутентификации, алгебраическая теория кодов и их применение в системах передачи данных.*